

## A Method and System for Performing Permutations Using Permutation Instructions Based on Modified Omega and Flip Stages

### Background of the Invention

*Application claims benefit of a provisional application N° 60/202,243*

#### 1. Field of the Invention      *Filed on 5/05/2000.*

The present invention relates to a method and system for performing arbitrary permutations of a sequence of bits in a programmable processor by determining a permutation instruction based on omega and flip networks.

#### 2. Description of the Related Art

The need for secure information processing has increased with the increasing use of the public internet and wireless communications in e-commerce, e-business and personal use. Typical use of the internet is not secure. Secure information processing typically includes authentication of users and host machines, confidentiality of messages sent over public networks, and assurances that messages, programs and data have not been maliciously changed. Conventional solutions have provided security functions by using different security protocols employing different cryptographic algorithms, such as public key, symmetric key and hash algorithms.

For encrypting large amounts of data, symmetric key cryptography algorithms have been used, see Bruce Schneier, "Applied Cryptography", 2nd Ed., John Wiley & Sons, Inc., 1996. These algorithms use the same secret key to encrypt and decrypt a given message, and encryption and decryption have the same computational complexity. In symmetric key algorithms, the cryptographic techniques of "confusion" and "diffusion" are synergistically employed. "Confusion" obscures the relationship between the plaintext (original message) and the ciphertext (encrypted message), for example, through substitution of arbitrary bits for bits in the plaintext. "Diffusion" spreads the redundancy of the plaintext over the ciphertext, for example through permutation of the bits of the plaintext block. Such bit-level